Understanding online safety through metaphors: UK policymakers and industry discourses about the internet

Article (Accepted Version)

Understanding online safety through metaphors: UK policymakers and industry discourses about the internet

Scholars analysing discourse around online risk and safety have often focused on the representation of (particularly young) internet users in public debate. A question that has received less attention in the literature is how online safety discourses conceptualise what the internet is. This article extends previous research, by exploring how key institutional participants in this debate use metaphors of the internet in their narratives about online safety. It suggests that metaphoric language that constructs the internet as a separate place from daily experience legitimises separate measures to control online risk and closes off possible connections with managing offline risk.

The study analyses policy discourse in a period when the UK government was preparing to introduce regulation against online harms. This was the first time the UK, or any major Western state, established direct regulation in this area. As will be discussed subsequently, the norm in Europe until the mid-2010s was self and co-regulation of the internet. The article analyses the government's proposal as well as documents by key players around the same period, to compare their discourse at this moment of veritable shift in policy.

The article uses discourse analysis to investigate how metaphor was used in selected documents published by the UK government, Ofcom (the UK's telecommunications regulator), and two Social Network Services (SNS) companies, which operate both in the UK and internationally. It suggests that these institutions do not construct online risk as a problem embedded in social experience, but as a phenomenon that happens

somewhere else, in a separate online space. I argue that this representation distances the problem from the real world and obscures its connection to behaviour in other realms of life. This is significant because our daily experience and interaction with the social world are increasingly mediated digitally (Fernback 2007; Carrington 2017).

Moreover, the article finds that whereas for the policy makers studied the solution lies in direct regulation of this online space, the SNS industry discourse views internet users as responsible for their own safety. This long-established liberal perspective has its roots in decades of self-regulation in this industry, but it clashes with the current move towards state intervention.

Regulation of the internet

Direct regulation, namely regulation of an industry by a state-appointed body that enforces its own legal rules (Marsden 2011), had not been a preferred option for regulating the internet in Europe until the mid-2010s. This was because state regulation was perceived as too rigid to respond to a complex and changing converged media sector, states were not perceived as having the insider knowledge to regulate the internet, whereas the global companies in this sector are not based within the jurisdiction of a single state (McLaughlin 2013).

Instead the preferred way of regulating the internet in its early years was self-regulation, where service providers and platforms collectively create their own codes of conduct and commit to upholding them – the industry itself creates and enforces the rules (Marsden 2011; McLaughlin 2013). Self-regulation measures to address

online risk include internet companies using software that detects and filters inappropriate content on their platforms, tools for users to report misconduct, human or automated content removal, help pages and educational material for users (deHaan et al. 2013). In SNSs' view, effective safety mechanisms teach users how to control their information sharing whilst maintaining freedom of speech (Jorgensen 2017); and have them moderate each other by signalling to the company which posted content is inappropriate, thus shifting the responsibility for identifying such content from the company to the user (Milosevic 2016, 5173). Indeed established SNSs' published guidelines often represent responsibility for user safety as a task shared between the SNS and the user community (Milosevic 2016). This rationale, argues Staksrud (2016), outsources responsibility for citizens' welfare from institutions to citizens themselves, denies them their citizen right to protection from harm, and makes it reliant on how they interact with the technology.

Self-regulation was the norm until the late 2000s, after which point Europe turned to co-regulation, whereby statutory regulators delegate responsibility for regulation to the industry but agree the rules with the industry and maintain an oversight of their implementation (Marsden 2011). This direction of travel from self-regulation towards gradually more involvement of the state seems to have continued, at least in the UK, in light of both the increasing role the internet plays in daily life and a decline of faith in self-regulation to alleviate online safety concerns.

In April 2019, a formal turning point for UK internet regulation policy, the Department for Digital, Culture, Media and Sport (DCMS) and the Home Office published the Online Harms White Paper, with its proposals to set out "the world's first framework

designed to hold internet companies accountable for the safety of their users" (Skelton 2020). Eventually this led to the appointment of Ofcom in late 2020 as a national regulator for online harms. Its role would be to shape rules on behalf of the state, monitor and oversee their enforcement by the industry, and apply sanctions.

Although this shift to direct regulation remains in progress at the time of writing, this article focuses on the period surrounding the publication of the White Paper. It aims to establish how metaphoric discourse both in the Paper and in publications by public bodies and industry players around that time may legitimise or oppose particular solutions. It looks at a key moment in the evolution of regulation and explores how discursive constructions of what the internet is have implications for how it is regulated.

Discourses of online safety

Much academic literature analysing online safety discourses focuses on the safety of young people, who are seen as particularly vulnerable. This research has found that public discourse emphasises the risks rather than the opportunities young people encounter online (Livingstone et al. 2018). Such risks include exposure to harmful or inappropriate *content* and *contact* with individuals who may harm them, but less attention is given to young people's own potentially problematic *conduct* online (Livingstone et al. 2014). Bulger et al (2017) suggest that internet safety discourse internationally has tended to view young people as innocent, in need of protection from risks and harms on digital platforms, but they argue that this fails to acknowledge evidence of young people's agency in these environments.

The same rationale that characterises broader public discourse is also reflected in media coverage of internet safety. Literature specifically analysing mediated discourse agrees that the mass media focus on the negatives and harms of the internet (Ponte et al. 2009; Haddon and Stald 2009), view internet users as “innocent” (Haddon and Stald 2009), “passive” (Ponte et al. 2009), potentially “untrustworthy” and in need of “monitoring” in an online environment (Fisk 2016; Hartikainen 2016), and only sometimes as potential “aggressors” (Ponte et al. 2009). The kinds of risks the media report tend to involve content and contact risks (Haddon and Stald 2009), as these were defined above. Experts and institutional voices are heard more often than users in media reports (Ponte et al. 2009; Hartikainen 2016).

However perceiving young people as active agents might be important when educating them on risk. Encountering risk can be essential in learning to protect oneself, scholars argue, and media literacy attempts should pay attention to how people deal with risk and develop the ability to cope (Staksrud and Livingstone 2009; Fisk 2016).

Similarly to the public and media discourses discussed above, policymakers broadly tend to see internet risks as isolated from young people’s social contexts. Livingstone et al. (2018) however stress that young people’s experience alters as the digital ecology changes and new generations have these technologies integrated into their lives at increasingly earlier stages. They call for research to focus “no longer [on users’] relationship with the internet as a medium but, more profoundly, [on] their relationship with the world as mediated by the internet in particular and changing ways” (Livingstone et al. 2018, 1117).

This article speaks to this context, by examining whether and to what extent the policy and industry discourses it analyses discuss online risk as part of users' relationship with the world. The article makes an original contribution by analysing metaphoric discourse to address this question. As seen in the literature reviewed above, previous research on internet safety discourses has described common themes within these discourses, but it has not looked at how their use of metaphor constructs this problem and its solutions. However, how we conceptualise solutions for online risk stems from how we understand what the internet is in the first place. The present article takes a step back to analyse policy and industry solutions within the context of what we know about different metaphoric ways of understanding the internet.

Metaphors and the internet

Lakoff and Johnson's (1980) cognitive linguistic theory of conceptual metaphor views metaphor not just as a figure of speech, but as a way of understanding concepts in day-to-day experience. This involves constructing one conceptual domain, namely the target domain, in terms of another, the source domain, from which vocabulary is borrowed and transferred. Their premise that people not only speak but also think of target domains in terms of source domains has been criticised on the grounds that such mappings are partial and not all properties of a domain are transferred to the target; that transferring vocabulary between domains does not necessarily reflect how these domains are mentally represented; or that more detail is needed to explain the mental processes involved in metaphorical mapping (see Thibodeau et al. 2019, for a detailed discussion). However several studies have collectively shown that, although

linguistic patterns cannot necessarily predict how people will behave, “metaphors can influence how people think about a wide range of sociopolitical issues” and do reflect patterns of thought (Thibodeau et al. 2019, 9).

Metaphor frames issues by selectively highlighting some of their aspects and concealing others and these frames can influence thinking within political and social institutions (Ryall 2008). Metaphors about technology have the potential to set the direction and the agenda for internet research and policy (Wilken 2013). For this reason, “it is crucial to re-examine our use of particular linguistic constructions in policy making” (Markham 2003,14).

Markham (2003) identifies three metaphors for understanding the internet – as a tool, as a place and as a way of being – which she suggests represent an evolution in how we experience it. Seeing the internet as a tool involves perceiving it as an extension of our physical selves, that allows us to do things like accessing information located far away. Seeing the internet as a place, involves understanding it as a separate environment where we interact “online”, beyond the physical world. A view of the internet as a way of being, by contrast, suggests that there is no distinction between living on and off line, as separate “places”, but the internet is just one “way one learns about, makes sense of, and ultimately knows the social world” (Markham 2003,10). This metaphor constructs the internet as one of the ways available to interact with others and do things, which is not separate from, nor less authentic than our offline experience (Markham 1998,168). Consequently, risks that we may face offline, such as scam, theft, terrorism or bullying, also exist online because they are part of the same social world.

Of these three metaphors, the one that constructs the internet as physical place has long been "fundamental to how virtual technologies are framed and understood" (Wilken 2007, 49). In the 1980s and 1990s, spatial metaphors became common in describing this new technology, for instance the information superhighway and cyberspace metaphors (Nunes 1995; Blavin and Cohen 2002). Each spatial metaphor has ideological implications for what can and should be done with the internet: the superhighway metaphor legitimates external regulation and emphasises the ephemerality of online content; whereas the cyberspace metaphor precludes regulation and emphasises the boundless nature of the internet (Blavin and Cohen 2002). Similarly, the metaphoric construction of the internet as a platform, which is common in the discourse of social media companies, emphasises its empowering, democratising role and, at the same time, limits these companies' liability for what is published on their "platforms", thus averting external regulation (Gillespie 2010). Indeed, as the above authors demonstrate, "in so far as metaphor is intertwined with rhetoric, metaphor is never innocent" (Wilken 2013, 642) because it is part of an attempt to persuade. Internet services that position themselves as platforms are not necessarily successful in avoiding regulation when political pressures prevail; indeed social media platforms are currently being targeted by European regulation. This though does not change the fact that the associations the platform metaphor carries are part of a rhetoric that attempts to deflect responsibility from these companies.

Although the superhighway and cyberspace metaphors became redundant over time, the internet as a separate physical space remains a dominant metaphor (Matlock et al. 2014). However, constructing the internet as separate from reality conceals that it

does not create problems that aren't also encountered in the real world (Blavin and Cohen 2002). Indeed as the internet gradually becomes central to how people do things in their daily lives, Blavin and Cohen (2002) predict a move towards a metaphor of the internet as "real space" (or as a way of being in Markham's terms). Nunes (1995, 317) goes further to suggest that the internet will one day replace real place and become "more real than real", as our experience of life is increasingly mediated through it. Mobile smart technology providing constant online access is already contributing to this (Wilken 2013).

Similarly, Carrington (2017) highlights that "online" and "offline" are themselves metaphors which are getting increasingly old, because the internet is no longer something we "connect" to some of the time via a modem, but it is there, "ready-to-hand", constantly. "All our lives are technologically mediated in some way" (Carrington 2017,17) and how we experience the world is partly constructed through technology.

Method

This article applies insights from the above research on internet metaphors to an analysis of current debates on online safety. It addresses two questions:

RQ1 Which metaphors inform the way policy makers and SNS companies discuss online safety in their respective documents? What does this reveal about how they understand potential solutions to online risk?

RQ2 Who do policy makers and SNS companies represent as responsible for addressing online risk?

It uses qualitative discourse analysis of documents produced around the period of the publication of the UK government's Online Harms White Paper. This was the first time the UK government proposed direct regulation of the internet and the article analyses the proposal itself, as well as material about online safety published by other public and private players in the period before/after this proposal. The purpose is to compare the discourse of the government at this official turning point to that of other players in the field in the same period. More specifically, this article analyses:

The UK government's **Online Harms White Paper**, presented to the UK Parliament in April 2019 by the Secretary of State for Digital, Culture, Media & Sport and the Home Secretary, setting out plans for establishing a new regulatory framework for online safety. These plans were subsequently put out for public consultation.

The UK's Office for Communications (Ofcom) **Addressing Harmful Content Online** paper, published in September 2018 and presenting the regulator's perspective on online safety regulation. Ofcom was at the time the regulator for UK broadcasting, and also the main candidate to be allocated the role of regulating online services.

The UK Council for Internet Safety (UKCIS) **Digital Resilience Framework**, published in September 2019. This aimed to help internet companies in supporting resilience to risk. The UKCIS is part of the government's Department for Digital, Culture, Media and Sport, but brings together technology companies, government and the third sector to cooperate on online safety. Its members include digital media companies such as Facebook and Google, as well as Ofcom and other key players.

All **press releases and blog posts** posted on the corporate websites of TikTok and Instagram, which had online safety as their subject and were published between May 2019 and February 2020.

All **videos** included under TikTok's "You're in control" online safety tag. These were published in November 2019 to educate users on TikTok's safety features.

These actors represent UK government, regulators, industry bodies and two major SNSs which operate both in the UK and globally. TikTok and Instagram were specifically selected due to their growing number of users in the period studied (Statista 2020a, 2020b) and their popularity among younger users (Ofcom, 2020), since the safety of young people is central to these debates.

All the content of the above documents was subjected to discourse analysis. As a qualitative method, discourse analysis works with small corpora and delivers an in-depth explanation of how language is used to reproduce a particular "system of values and beliefs" (Scannel 1998, 256). It is not about measuring or statistically representing elements of texts but about interpreting them: the researcher's task is to build a convincing explanation of the text based on theoretical and empirical arguments (Chouliaraki and Fairclough, 1999). Its validity relies on the systematic application of the analytical tools chosen, on citing excerpts to back up the inferences made, on reporting any instances that contradict these inferences, and on providing a convincing account with evidence from the analysed texts (Lincoln and Guba, 1985).

My analysis focused on two aspects of the language used: metaphor analysis (Charteris-Black 2011) and an analysis of transitivity (Richardson 2007). Metaphor analysis is based on Lakoff and Johnson's (1980) cognitive linguistic theory of metaphor, reviewed in the previous section. I followed Charteris-Black's (2011) empirical approach: this involves reading each text carefully and systematically identifying every instance where words or phrases are used with a non-literal meaning; then identifying the source domains these were taken from and mapping the correspondences between source and target domains (Charteris-Black 2011). The target domain I focused on was the internet, so I mapped all metaphoric expressions about it to their corresponding source domains. I classified together all excerpts where the same source domain was used (instances of the same metaphor) and I present the metaphors I identified in the first two findings sections below. I use excerpts from among those classified under each metaphor to illustrate how the metaphor typically appears in the texts. Conceptual metaphors are in small caps, as is conventional in cognitive linguistic theory (Lakoff and Johnson, 1980).

An analysis of transitivity involves systematically identifying all the verbs used in a text, and their syntactic subjects and objects. This is done to discuss who is presented as doing what to whom, who is in subject position controlling action and is thus represented as powerful, and who is affected by the actions of others (Richardson 2007; Fowler 1991). In each of the analysed texts, I identified the syntactic positions occupied by the main actors in the safety debate (internet users, regulators and the government) in every sentence they were mentioned, I grouped together excerpts where the same actors held the same syntactic positions, and I thus identified patterns

in the different texts. I discuss these patterns in the third findings section below, and I present typical examples illustrating them.

FINDINGS

The internet as a place

The first finding of the analysis is that the internet is not represented as “a way of being” (Markham 2003) by most of the actors involved in addressing online risk. Although the internet is increasingly an integral part of everyday life, the main metaphor used to describe it in the discourse of policymakers, regulators and the industry is that of a place. Going to this “online place” implies that it is located separately from offline experience (to “go” somewhere presupposes leaving another place behind) and, in this way, the discourse analysed conceals the possibility that the risks that exist online may be rooted in the “offline world”.

The metaphor of the internet as a separate place (THE INTERNET IS A PLACE) is dominant across all the material analysed. For instance, the Online Harms White Paper suggests that: “illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet” (2019, 5). “Online” and “on the internet” in this excerpt indicate a place where people go and encounter “illegal and unacceptable” content. This leaves them “concerned”, presumably because such content is unusual in their offline experience.

Similarly, the White Paper also warns that “if we surrender our online spaces to those who spread hate, abuse, fear and vitriolic content, then we will all lose” (2019, 3). In this instance of the place metaphor, it is combined with a war metaphor, whereby the internet is represented as a land that can be “surrendered” to an enemy. The enemy is those who cause online risk (“those who spread hate, abuse, fear and vitriolic content”) and any attempts to deal with online risk are thus constructed here as a war against these anonymous individuals. The war metaphor serves to evoke a threat “that must be curbed by human intervention”, which is a common rhetorical technique in political discourse around technology (Pushman and Burgess 2014, 1697).

Further examples of the place metaphor can be found in Ofcom’s Addressing Harmful Online Content report, where “a debate is underway about whether regulation is needed to address a range of problems that originate online” (2018,1). “Online” again is a linguistic indicator of place in this excerpt, and this time this place is a breeding space for problems. Later in the same report, the internet is constructed as not just a separate place, but a completely different world: “existing frameworks could not be transferred wholesale to the online world” (Ofcom 2018, 4).

In line with the two policymakers’ documents above, the industry documents also metaphorically construct the internet as a distinct place. However, whereas in the policy documents this place is presented as rather negative, problematic and risky, as was seen in the earlier examples, in the industry material the dominant version of the place metaphor is that of a more positive “environment”:

> “people socialise, explore, create and work in digital environments” (UKCIS 2019, 1)
>
> “our Community Guidelines support a safe and open environment for everyone” (Instagram 2020a)
>
> “our platform empowers users to express themselves, inspire others, and have fun in a safe and welcoming environment” (TikTok 2019b).

Understandably, in the above examples the industry itself sees the internet as a place for self-expression and entertainment, rather than a breeding ground for negative experiences. In line with this more favourable deployment of the place metaphor, the industry documents also use the spatially-based metaphor THE INTERNET IS A COMMUNITY – for example in the second excerpt above. This metaphor involves a focus not on the geographical but the social aspect of place, the coming together of people to form a cohesive group (Fernback 2007). This positive construction of the internet in these documents does not however mean that the industry fails to acknowledge the presence of risk online, as will be discussed in a later section.

The only material analysed where the construction of the internet as a separate place is challenged are the “You’re in control” videos that TikTok uses to promote online safety among its young users. Similarly to the examples analysed so far, these videos also feature THE INTERNET IS A PLACE metaphor. However this place is here constructed in terms of day-to-day “offline” experience, *not* as different from it. TikTok’s videos are mostly silent and feature short scenarios metaphorically presenting online risk as annoying situations in everyday places. One of the characters has popcorn thrown at them at a party, another is annoyed by a fellow passenger putting up their smelly feet

on a bus seat (Figure 1), a further character is intimidated by a large dog (Figure 2). These pests represent unsolicited messages, offensive behaviour or bullying online.

INSERT FIGURE 1 HERE

INSERT FIGURE 2 HERE

By contrast to the previous examples, the spatial metaphor here connects online and everyday experience. These instances are the closest any of the analysed material came to THE INTERNET IS A WAY OF BEING metaphor, as these videos invite users to "experience life and technology on the same plane" (Markham 2003,10). At the same time however, the videos trivialise online risk by making analogies with comical offline experiences (smelly feet, scary dog), which play down online harms' seriousness and impact on victims.

The solutions given in the videos are initiated either by the recipient of the annoying behaviour or their peers: a bus driver throws a pair of shoes for the offender to cover their bare feet, another character throws negative words down a toilet. Internet users are represented as in control of their own and each other's experience. This is consistent with SNS's longstanding approach to online safety, as discussed in an earlier section, and is an example of a tendency to outsource institutional responsibility for reducing risk to citizens, positioning them as making decisions previously made by institutions, and making it their fault if they fail to protect themselves (Staksrud, 2016). They may be granted agency, but they are also treated as consumers of a product,

not as citizens who have a right to be protected from harm (Milosevic 2016; Staksrud 2016).

The internet as tool

A second finding of the analysis is that the UK government's White Paper, setting national policy on internet safety, constructs the internet as a tool that may fall in the wrong hands and be used to harm. This is significant because framing the internet in such a way portrays risk as intentionally caused by wrongdoers who take advantage of the "tool" to harm innocents, and not as something that emerges from social behaviour. As such, the government adopts an understanding of online harm as an external threat to (British) users and not as something they may cause themselves.

THE INTERNET IS A TOOL metaphor deployed in the White Paper represents the internet as an "extension or prosthesis" (Markham 2003) which allows wrongdoers to extend the reach of their evil acts across geographical distance. For example, in one of the instances of the metaphor in the Online Harms White Paper:

> "Online services can be used to spread terrorist propaganda and child abuse content, they can be a tool for abuse and bullying, and they can be used to undermine civil discourse" (2019, 12).

This metaphor transfers to the internet qualities normally associated with a tool: it helps materialise the intentions of its user and directly affects those on whom it is used, in the way that the user intends it to. The metaphor thus carries over connotations of

control and domination (Warnick 2004) into the target domain of the internet. It also carries over the expectation that, like a tool, the internet was created with some specific purpose to fulfil (ibid) and other uses of it are wrong.

The metaphor additionally allows the document to construct an anonymous enemy who uses this manipulatable “tool” to threaten national safety. In other instances of this metaphor, the Online Harms White Paper states that the internet “can be used to undermine our democratic values” (2019, 5); “threaten our national security” (2019, 11); or “threaten our way of life in the UK” (2019, 30). The identity of this threatening enemy is concealed through agentless passive voice and nominalisations, but the discourse creates an entity for the British government to fight against and thus legitimises punitive legislation.

This understanding of the internet as a potentially dangerous tool in the wrong hands precludes an understanding of online risk as part of societal behaviour. The tool metaphor “separate[s] the technology from its users as well as from the contexts of its use” (Koteyko et al. 2015, 480). Users of the internet are absent in the example above and have no agency over the “spread of terrorist propaganda”, “abuse and bullying”, or over what happens to “civil discourse”.

Taking action against online risk

The previous sections established that in the analysed documents online risk is constructed as something happening in a separate place from ordinary experience,

and as a misuse of the internet by an enemy that needs to be fought against. This section will explore who is represented as responsible to undertake this “fight”.

Policy makers and the industry have divergent views on this matter, as these emerge from the analysis of their respective documents. Whereas for policy makers the solution lies in government initiative and legislation, in the industry documents internet users have more agency, supported by the SNS companies themselves.

In the Online Harms White Paper, the British government is constructed as the main agent taking action against online risk. Although there are some instances in this discourse where regulators and internet companies are also presented as having some responsibility, this is presented as a result of the government mobilising them. For instance:

> “This White Paper sets out government action to tackle online content or activity that harms individual users, particularly children, or threatens our way of life in the UK” (2019, 30).

> “The government will establish a new statutory duty of care on relevant companies to take reasonable steps to keep their users safe and tackle illegal and harmful activity on their services” (2019, 42).

The main actor controlling action verbs in the two excerpts above is the government (and its White Paper via metonymy). This actor is responsible “to tackle” online risk, and to “establish” a duty for internet companies. In the second example, companies

appear in subject position of action verbs too (“take steps”, “keep”, “tackle”) but these are all in secondary clauses, resulting from the action of the government (“establish a statutory duty”).

The role of internet users in the Online Harms White Paper is overall limited. Users appear rarely in the document as subjects of verbs - they are usually affected by the actions described in sentences. For example:

> “All users, children and adults, should be empowered to understand and manage risks so that they can stay safe online” (2019, 85).

> “This White Paper sets out a programme of action to tackle content or activity that harms individual users” (2019, 6).

In the first example above, users are the subject of an agentless passive (“should be empowered”) and the active voice verbs “understand” and “manage”. Although they are positioned as “managing” their online experience, this is not possible unless another nameless agent enables them (“should be empowered to”). Besides “empower” triggers the presupposition that users are currently powerless. In the second example, as in many others in the document, users are the object of a verb (“harms”) controlled by other actors, in this case by the nominalisations “content” and “activity”. On the few occasions in this document where internet users are subjects of verbs, these are thought processes (such as “understand” of “feel”) but never action verbs. The document does not assign internet users agency over their safety.

In Ofcom's Addressing Harmful Online Content document, legislation and regulation are the agents responsible for dealing with online risk. Once again, internet users are powerless. Heavy use of nominalisations excludes human agents from the narrative, but the implied agents responsible are governments and regulators. For example:

> "New European legislation will increase the level of regulation of online video content" (2018, 19).

> "We also cover how regulatory and voluntary initiatives have developed various protections in certain parts of the online world" (2018, 14).

In both the above excerpts, nominalisations replace human agents ("legislation", "regulatory and voluntary initiatives") as subjects of action verbs ("will increase", "have developed"). The implied human agents are legislative authorities. Moreover, and similarly to the government, Ofcom's document constructs the public as passive in regards to its own safety:

> "But there is an intensifying, global debate over how to address the various problems that people experience online" (2018,3).

> "However, users should be able to trust or, at least, critically assess the factual content they view online. People should be able to know who has created the content they see" (2018, 30).

In the examples above, users are the subject of mental state/action verbs ("experience", "trust", "assess", "know") but don't yield any power over their online experience. Here users are constructed as in control of what they think, but not in a position to do anything about their safety.

Responsibility for causing online risk is not attributed to anyone in Ofcom's Addressing Harmful Content document. Nominalisations ("bullying", "harassment", "conduct") replace human agency wherever online risk is mentioned, thus avoiding to identify who does these actions. For example, "personal conduct that is illegal or harmful - such as bullying, grooming and harassment" (Ofcom 2018,12) does not reveal who is the agent of the "conduct", "bullying", or "grooming" referred to. This contrasts with the discourse of the White Paper examined earlier, which attributes online harms to an enemy of the nation. For Ofcom, online harms are therefore represented as phenomena (nouns) rather than as actions (verbs).

Clearly neither Ofcom nor the UK Government regulate individuals' behaviour online. These actors' remit is to regulate the SNS industry, which then enforces measures on users. This may to an extent justify why users don't feature as powerful actors in regulators' documents though, that said, the SNS industry does not feature as very powerful either. These documents place policymakers or regulation as key agents in securing safety, thus helping to reinforce the need for external regulation.

By contrast to the government and Ofcom documents, which represent users as broadly powerless over their own safety, the SNSs' press releases and safety-themed blogs position them in control of their experience:

> “Your teen's account can be set to private, meaning their content will only be seen by approved followers. They can also block and report abusive accounts” (Instagram 2020b).

> “It’s also important for our community to look after their wellbeing, which means having a healthy relationship with online apps and services” (TikTok 2020)

In these examples, internet users are in subject position of physical action verbs (“block”, “report”, “look after”) affecting themselves and their peers. They are thus positioned as powerful actors who can take action to protect themselves against risk. Both platforms’ discourse also features several instances where the SNS is in control of action that assists users in their effort to protect themselves. For example:

> “In addition to features that help you stand up to bullying, we've created new ways to help stop bullying before it happens” (Instagram 2020c).

In this excerpt the SNS controls action (“help”) which has users as its object and allows them to carry out the action that they control in the secondary clause (“stand up”). Although the user is still responsible for standing up to bullying, the SNS contributes to this task and controls three action verbs (“help”, “created”, “stop”). Online safety is thus a collaboration between companies and users, where the former enable the latter. Established SNSs often represent responsibility for user safety as shared between the SNS and the user community: previous research revealed that SNSs view user

communities moderating themselves as “an advanced or evolved self-regulatory mechanism”(Milosevic 2016, 5174). This tendency to shift responsibility was formed over years of industry self-regulation, as discussed earlier, but clashes with the discourse of direct regulation found in the policymakers’ documents, which place responsibility on institutions and not on users.

Finally, responsibility for *causing* online risk is attributed differently in the discourse of the two SNS companies: Instagram sometimes attributes responsibility to users for causing harm, whereas TikTok avoids this. Like in Ofcom’s document, TikTok’s press releases and safety blogs do not present users themselves as causing online harms:

> “Harmful or dangerous content, violence, discrimination or hate speech, abuse or sexual activity, harassment or cyberbullying, and misleading content has no place in the TikTok community” (TikTok 2019a)

Wherever TikTok refers to harmful behaviour, this is in nominalisations (“content”, “violence”, “discrimination”, “speech”, “abuse”, “activity”, “harassment”, “cyberbullying” in the example above). Using these nouns, instead of the equivalent verbs, represents these behaviours as phenomena rather than as someone’s deliberate action. By contrast, Instagram occasionally attributes harmful behaviour to its own users:

> “Young people face a disproportionate amount of online bullying but are reluctant to report or block peers who bully them, so last year we created a new feature called Restrict” (Instagram 2020c).

“Peers who bully them” directly attributes responsibility not to some enemy, like the government’s White Paper did earlier, but to ordinary users. This avoids representing bullying as an abstract phenomenon and is consistent with viewing it as part of social behaviour, perhaps not too dissimilar to real-life bullying.

Conclusion

Metaphors open up ways of thinking about things by making connections of analogy between these things and originally unrelated domains of our experience (Lakoff and Johnson 1980). At the same time though, when a metaphor becomes the standardised way of speaking about an issue, it constructs a system of meaning that pushes back other ways of understanding this issue. Spatial metaphors of the internet originate in a time when it was a relatively new technology (Nunes 1995), that people accessed some of the time to seek information or to have interactions “somewhere else”. However, thinking about going online as going to another place discourages an understanding of what happens there as behaviour that is also encountered offline.

This article has found that an understanding of the internet as a place separate from the ‘real’ world remained dominant in official discourse at a time when the UK was taking a major step towards direct regulation of the industry. Moreover it found that UK legislators specifically also viewed the internet as a tool that could fall into the wrong hands and be used for harm. Such constructions legitimise rules to control this online “place” and institutions to “punish” those who intentionally cause harm.

The metaphor of the internet as a separate place was common across both the policymakers' and industry documents. One of the SNSs used the internet "as a way of being" (Markham, 2003) metaphor, but only in videos addressing its users. The fact that, as opposed to policymakers, SNSs have a responsibility to set rules directly for individuals may have influenced this but, even so, this metaphor was relatively rare.

Place and tool metaphors encourage a view of online risk as having different qualities from risk in everyday life. They discourage policymakers, regulators and the industry from assessing what learnings can be transferred from dealing with harms in other realms of life. These discourses therefore restrict policy interventions by obscuring the possibility that doing harm online might be one way people do harm within the social world and addressing it might involve exploring causes and solutions in society.

The solutions encouraged by the place and tool metaphors are punitive and top-down. Dealing with risk people encounter in a place foreign to their ordinary experience, or stopping evil wrongdoers using a potentially dangerous tool against the powerless both require strict rules to be set and implemented by policing institutions. Intervening to prevent people harming others as part of everyday interactions would involve engaging with users, consulting them and understanding how these interactions work.

In general the documents analysed either present the perpetrators of online harms as enemies of the state (the White Paper), or don't even refer to them as human actors. Online harms are often written about as phenomena without agents. This makes it difficult to see them as behaviours that need to be comprehended in order to resolve.

In addition, the findings suggest that the discourse of UK policymakers veers away from the industry's perspective that puts responsibility for online safety on the end user. This approach is well-established among SNSs and it is how the industry has traditionally managed self-regulation of online safety (Jorgensen 2017; Milosevic 2016). However the policymakers' documents examined here put responsibility on the state and regulators for addressing online harms and protecting users' rights. This discrepancy between companies' neoliberal and legislators' interventionist discourse might suggest a disconnect between them, as the UK proceeds with direct regulation.

In an era when the internet is constantly available and we live and manage interpersonal and professional relationships through it (Blavin and Cohen 2002; Carrington 2017), the distinction between online and offline is perhaps more blurred than the analysed documents may suggest. Our social world is experienced through multiple means, some of them physical and some digitally mediated. Perhaps this interconnectedness could also extend to thinking about preventing or addressing risk.

References

Blavin, Jonathan and Glenn Cohen. 2002. "Gore, Gibson, and Goldsmith: The evolution of internet metaphors in law and commentary." *Harvard Journal of Law & Technology* 16(1): 265-286.

Bulger, Monica, Burton, Patrick, O'Neil Brian and Elisabeth Staksrud. 2017. "Where policy and practice collide: comparing United States, South African and European Union approaches to protecting children online". *New Media and Society* 19(5): 750-764.

Carrington, Victoria. 2017. "How we live now: 'I don't think there's such a thing as being offline'". *Teachers College Record* 119(12): 1-24.

Charteris-Black, Jonathan. 2011. *Politicians and Rhetoric: the Persuasive Power of Metaphor*. Second edition. Basingstoke: Palgrave Macmillan.

Chouliaraki, Lilie and Fairclough, Norman. 1999. *Discourse in Late Modernity*. Edinburgh: EUP.

deHaan, Jos, van derHof, Simone, Bekkers, Wim, and Pijpers, Remco. 2013. "Self-regulation". In O'Neil, Brian, Staksrud, Elisabeth and McLaughlin, Sharon (eds). *Towards a Better Internet for Children? Policy Pillars, Players and Paradoxes*. Goteborg: Nordicom, pp.111-129.

Fernback, Jan. 2007. "Beyond the diluted community concept: a symbolic interactionist perspective on online social relations". *New Media and Society* 9(1): 49-69.

Fisk, Nathan. 2016. *Framing Internet Safety: the Governance of Youth Online*. Cambridge, MA: MIT Press.

Fowler, Roger. 1991. *Language in the News*. London: Routledge.

Gillespie, Tarleton. 2010. “The politics of platforms”. *New Media and Society* 12(3): 347–364.

Haddon, Leslie and Gitte Stald. 2009. “A comparative analysis of European press coverage of children and the internet”. *Journal of Children and Media* 3(4): 379-393.

Hartikainen, Heidi, Iivari, Netta and Marianne Kinnula. 2016. “Should we design for control, trust or involvement? A discourses survey about children’s online safety”. *IDC* 367-378.

Instagram. 2020a. “Keeping Instagram a safe and supportive place”. Available from: https://about.instagram.com/community/safety (accessed 7.6.2020).

Instagram. 2020b. “Helping your teen navigate Instagram safely”. Available from: https://about.instagram.com/community/parents (accessed 7.6.2020)

Instagram. 2020c, 11 February. “#SaferInternetDay”. Available from: https://about.instagram.com/blog/announcements/safer-internet-day-2020 (accessed 7.6.2020).

Jorgensen, Rikke. 2017. “What platforms mean when they talk about human rights”. *Policy and Internet* 9(3): 280-296.

Koteyko, Nelya, Hunt, Daniel and Barrie Gunter. 2015. “Expectations in the field of the internet and health: an analysis of claims about social networking sites in clinical literature”. *Sociology of Health and Illness* 37(3): 468–484.

Lakoff, George and Mark Johnson. 1980. *Metaphors we Live by*. Chicago: University of Chicago Press.

Lincoln, Yvonna and Guba, Egon. 1985. Naturalistic Inquiry. Beverly Hills: Sage.

Livingstone, Sonia, Mascheroni Giovanna, Ólafsson Kjartan and Leslie Haddon. 2014. *Children’s Online Risks and Opportunities: Comparative Findings from EU*

Kids Online and Net Children Go Mobile. London: EU Kids Online and Net Children Go Mobile.

Livingstone, Sonia, Mascheroni Giovanna and Elisabeth Staksrud. 2018. “European research on children’s internet use: assessing the past and anticipating the future”. *New Media and Society* 20(3): 1103–1122.

Marsden, Christopher. 2011. *Internet Co-regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*. Cambridge: CUP.

McLaughlin, Sharon. 2013. Regulation and legislation. In O’Neil, Brian, Staksrud, Elisabeth and McLaughlin, Sharon (eds). *Towards a Better Internet for Children? Policy Pillars, Players and Paradoxes*. Goteborg: Nordicom, pp. 77-92.

Markham, Annette. 1998. *Life Online: Researching Real Experience in Virtual Space*. AltaMira Press.

Markham, Annette. 2003. “Metaphors reflecting and shaping the reality of the internet: tool, place, way of being”. Paper presented at the Association of Internet Researchers Conference, Toronto Canada. Available from: http://markham.internetinquiry.org/writing/MarkhamTPW.pdf (accessed 7.6.20)

Matlock, Teenie, Castro, Spencer, Fleming, Morgan, Gann, Timothy and Paul Maglio. 2014. “Spatial metaphors of web use”. *Spatial Cognition & Computation* 14(4):306-320.

Milosevic, Tijana. 2016. “Social media companies’ cyberbullying policies”. *International Journal of Communication*, 10: 5164-5185.

Nunes, Mark. 1995. “Jean Baudrillard in cyberspace: Internet, virtuality, and postmodernity”. *Style* 29(2): 314-327.

Ofcom. 2018, 18 September. “Addressing harmful online content”. Available from: https://www.ofcom.org.uk/__data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf (accessed 7.6.2020)

Ofcom. 2020, 24 June. “Adults’ media use and attitudes”. Available from: https://www.ofcom.org.uk/__data/assets/pdf_file/0031/196375/adults-media-use-and-attitudes-2020-report.pdf (accessed 20.12.2020)

Online Harms White Paper. 2019, April. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf (accessed 7.6.2020)

Ponte, Christina, Bauwens, Joke and Giovanna Mascheroni. 2009. “Children and the internet in the news: agency, voices and agendas”. In *Kids Online: Opportunities and Risks for Children,* edited by Sonia Livingstone and Leslie Haddon, 159-171. Bristol: Bristol University Press.

Puschmann, Cornelius and Jean Burgess. 2014. “Metaphors of big data”. *International Journal of Communication* 8:1690–1709

Richardson, John. 2007. *Analysing Newspapers: an Approach From Critical Discourse. Analysis*. Basingstoke: Palgrave MacMillan.

Ryall, Emily. 2008. “The language of genetic technology: Metaphor and media representation”. *Continuum* 22(3): 363-373.

Scannel, Paddy. 1998. “Media-language-world”. In Bell, Allan and Garret, Peter (eds). *Approaches to Media Discourse*. Malden:Blackwell, pp. 251-267.

Skelton, Sebastian Klovig. 2020, 15 December. “UK government unveils details of upcoming online harms rules”. *Computer Weekly*. Available from: https://www.computerweekly.com/news/252493664/UK-government-unveils-details-of-upcoming-online-harms-bill (accessed 15.12.2020).

Staksrud, Elisabeth. 2016. *Children in the Online World: Risk, Regulation, Rights*. London: Routledge.

Staksrud, Elisabeth and Sonia Livingstone. 2009. “Children and online risk”. *Information, Communication & Society* 12(3): 364-387.

Statista. 2020a. “United Kingdom: monthly Instagram users 2018-2020”. Available from https://www.statista.com/statistics/1018494/instagram-users-united-kingdom/ (accessed 20.12.2020).

Statista. 2020b. “Monthly active users of TikTok in the UK 2017-2020”. Available from https://www.statista.com/statistics/1125306/tiktok-monthly-active-users-uk/ (accessed 20.12.2020).

Thibodeau, Paul, Matlock, Teeny and Steven Flusberg. 2019. “The role of metaphor in communication and thought”. *Language and Linguistics Compass* 13: e12327.

TikTok. 2019a, 2 May. “TikTok glossary part 1”. Available from: https://newsroom.tiktok.com/en-gb/tiktok-glossary-1 (accessed 7.6.2020).

TikTok. 2019b, 3 December. “Updating our gifting policies to protect our community”. Available from: https://newsroom.tiktok.com/en-gb/updating-our-gifting-policies (accessed 7.6.2020).

TikTok. 2020, 19 February. “Introducing Family Safety Mode and Screentime Management in Feed”. Available from: https://newsroom.tiktok.com/en-gb/family-safety-mode-and-screentime-management-in-feed (accessed 7.6.2020).

UKCIS. 2019, 12 September. “Digital resilience framework”. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf (accessed 7.6.2020)

Warnick, Bryan. 2004. “Technological metaphors and moral education: The hacker ethic and the computational experience”. *Studies in Philosophy and Education* 23: 265–281.

Wilken, Rowan. 2007. “The haunting affect of place in the discourse of the virtual”. *Ethics Place and Environment* 10(1): 49-63.

Wilken, Rowan. 2013. “An exploratory comparative analysis of the use of metaphors in writing on the internet and mobile phones”. *Social Semiotics* 23(5): 632-647.

Figure 1. TikTok Tips – 2019.10.23. Available at: https://www.tiktok.com/@tiktoktips/video/6751042775589948678?enter_from=h5_m&is_copy_url=0&is_from_webapp=v1&sender_device=pc&sender_web_id=6992181168834708997

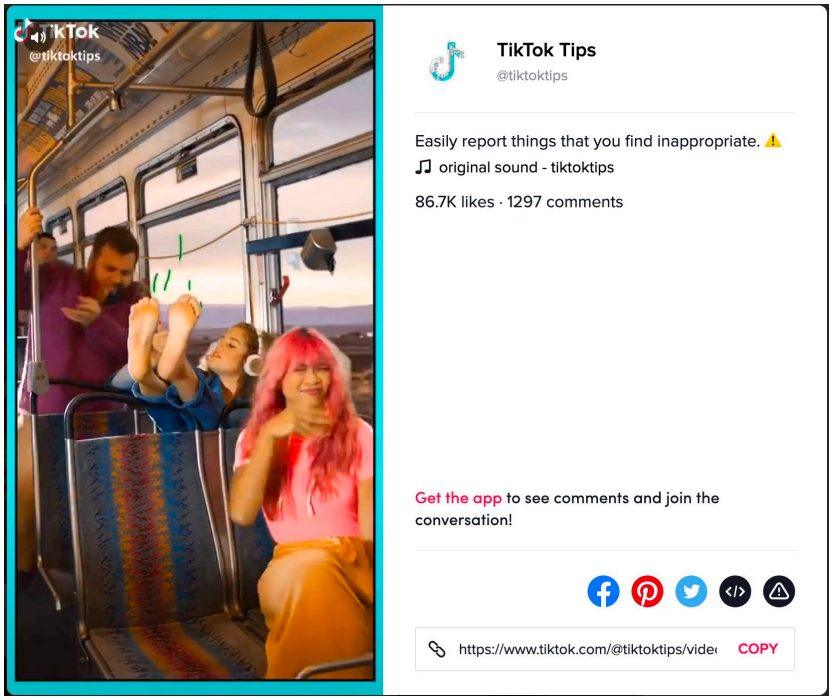

Figure 2. TikTok Tips – 2019.02.26. Available at: https://www.tiktok.com/@tiktoktips/video/6662444458073656582?enter_from=h5_m&is_copy_url=0&is_from_webapp=v1&sender_device=pc&sender_web_id=6992181168834708997